EMERALD

ITO

Monitor API
(Correlation of External Results)

Monitor API
(Results Dissemination)

RESOLVER

Monitor API

RESOURCE OBJECT

PROFILER ENGINES

SIGNATURE ENGINES

Monitor API
(Event Reporting)

SMTP FTP DNS NFS

New Technical Ideas
(http://www.csl.sri.com/intrusion.html)

- Heterogeneous signature-based and statistical analysis at multiple layers of abstraction

- Analysis target-independent code-base, with pluggable *resource-object* libraries.

- Hierarchical system layerability, with coordinated aggregate analyses

- Subscription-based (push/pull) message interface with support for third-party interoperability

Impact

- Ability to analyze and interpret system and network
  misuse

- Interoperability, reusability, rapid integration,
  evolvable, CIDF compliance

- Highly extensible analytical techniques to other
  application domains (e.g., survivability, fault tolerance, reliability.)

- Unprecedented scalability

Schedule

Integrated Expert & Statistical Anomaly Detection Services with Correlator

Expert system, resolver, service-layer analysis

Emerald design, new statistics component

Yr: ●●●●●●●●●1 ●●●●●●●●● 2 ●●●●●●●●●3